Cybersecurity – Appendix E Shipboard Example

<The following information is provided in Appendix E only if not already included in the body of the TEMP. The cybersecurity information need not be duplicated in both places.>

The Operational Test Agency (OTA) will perform cybersecurity testing as part of OT&E for the Shipboard Integrated Mission System (SIMS) in accordance with 1 Aug 2014 DOT&E guidance. Prior to these tests, SIMS will have a signed Authority to Operate.

E.1. System Description A unit equipped with SIMS is able to employ multiple systems from integrated control operator consoles. SIMS consoles have access to both NIPRNet and SIPRNet. The consoles provide a human interface to sensors, weapons, and systems required to safely operate the ship, including network accessible Programmable Logic Controllers (PLCs) and other industrial controls systems for propulsion and electrical distribution. Units equipped with SIMS perform cyber defense functions interoperating with the Navy Cyber Defense Operations Command (NCDOC) for both unclassified and secret networks.

E.2. System Threats A full range of cyber adversaries with nascent, limited, moderate, and advanced capabilities will target the SIMS. Adversaries will attempt to compromise the system; exfiltrate, infiltrate, or corrupt data; disrupt system operations; and, if possible, physically destroy equipment. Additional cyber threat information on the SIMS is provided in the SIMS System Threat Assessment Report (STAR) and the Computer Network Operations Capstone Threat Assessment (IO Capstone, Volume 10) (CORRECTED), 2nd Edition, May 2013, DIA-08-1209-908.A.

E.3. SIMS Architecture and Test Boundary

SIMS comprises servers, computers / consoles, and other networked devices hosted aboard a ship with unclassified and secret enclaves (see Figure E-1). In both enclaves, there are servers for databases, SIMS services, and SIMS operator-facing control consoles. The unclassified SIMS enclave includes connectivity to NIPRNet, various sensors, systems, and physical media devices, and provides data transfer capability via SIMS consoles. The unclassified enclave also has connectivity to the secret enclave via an approved cross-domain solution.

In addition to the unclassified data that arrives via the cross-domain solution, the secret enclave receives data via the SIPRNet, connected sensors and systems, and physical media devices. Like the unclassified version, the secret enclave has consoles to enable secret processing and telecommunication.

The architecture, proposed test boundary for the CVPA and AA, and external interfaces of the SIMS are shown in Figure E-1.

In typical operations, cyber defense for the SIMS is provided locally (Tier 3) by the system operators and system administrators, including a contingent of sustainment support from the development contractor. The Navy Cyber Defense Operations Command (NCDOC) in

Norfolk, Virginia is the Tier 2 Computer Network Defense Service Provider (CNDSP)[1] for both the unclassified and secret networks.

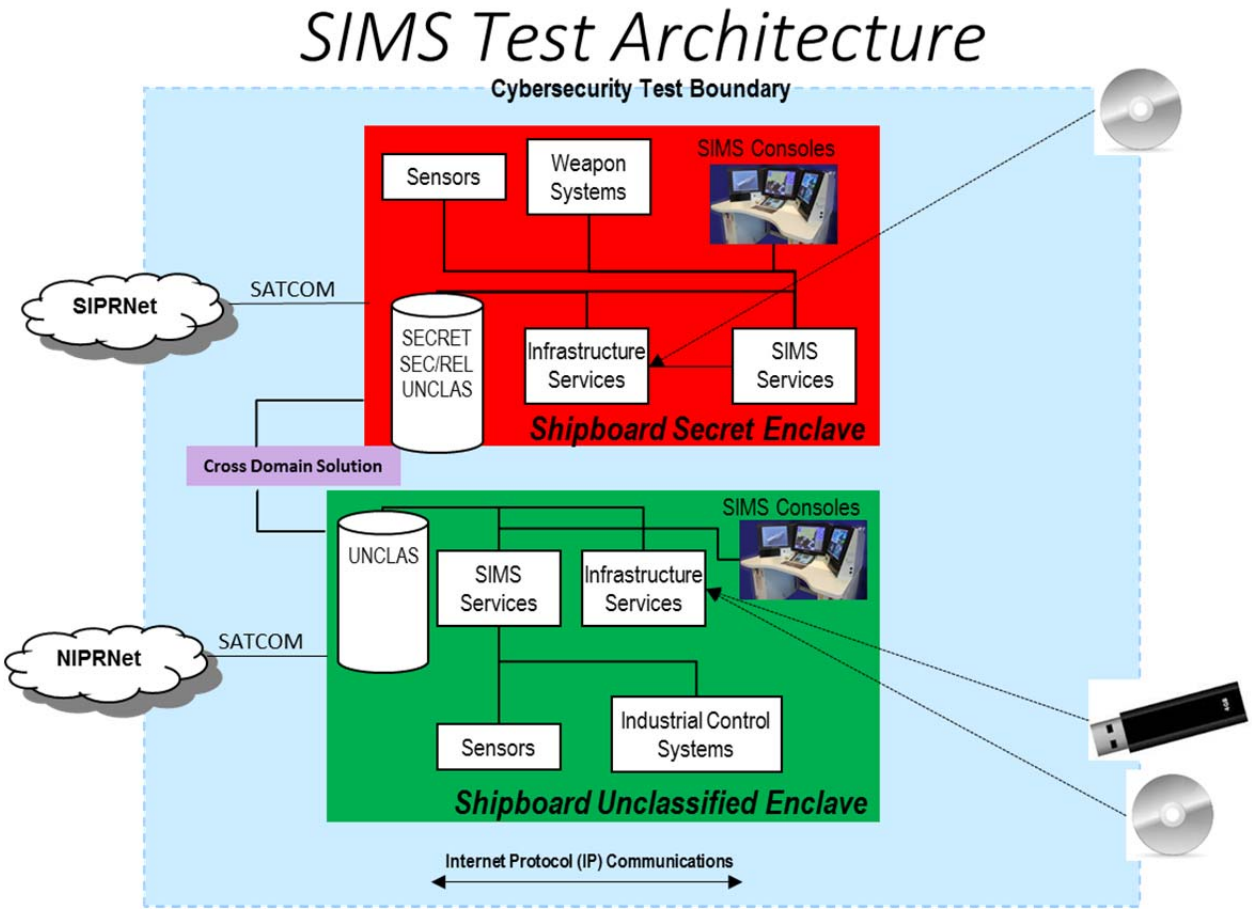

Figure E-1. SIMS Test Architecture

E.4. Cooperative Vulnerability and Penetration Assessment (CVPA). The OTA will employ a combined Navy Information Operations Command (NIOC) and Commander Operational Test and Evaluation Force (COMOPTEVFOR) cyber team to perform the Cooperative Vulnerability and Penetration Assessment (CVPA) during the OA. NIOC/COMOPTEVFOR will perform the CVPA on an operationally representative SIMS, including local cybersecurity defenders such as system operators and system administrators to support data collection (e.g., through interviews), while the ship is in port during a pre-deployment time period when all ship systems will be present and powered. NIOC/COMOPTEVFOR will execute vulnerability and penetration testing using their accredited tools and processes, which include automated scans and manual inspection. The SIMS will have all external interfaces active, and NIOC/COMOPTEVFOR will conduct assessment activities from the insider, outsider, and nearsider postures; the proposed test boundary is shown in Figure E-1. NIOC/COMOPTEVFOR will collect, at a minimum, the data in Attachments A and B of DOT&E guidance. NOIC/COMOPTEVFOR will provide a full

[1] Sometimes called Cybersecurity Defense Service Provider (CDSP)

report and all data to DOT&E within 45 days of the assessment. Resources required for this test can be found in Table E-1. The OTA will submit the CVPA test plan to DOT&E for approval 90 days prior to execution.

E.5. Adversarial Assessment (AA). The OTA will conduct an Adversarial Assessment (AA) during the IOT&E using a combined NIOC/COMOPTEVFOR cyber team led by NIOC, who will portray the cyber threat. NIOC is an NSA-certified, USCYBERCOM-accredited cyber threat team. NIOC/COMOPTEVFOR will execute the AA using their accredited tools and processes and portray a cyber threat (insider, nearsider, and outsider) in accordance with the STAR and the DIA Computer Network Operations Capstone Threat Assessment. The OTA will conduct the assessment in the context of SIMS mission operations, with representative data sources, network traffic, and external interface connectivity; the proposed test boundary is shown in Figure E-1. The assessment will include operationally representative network defense, including the local user and administrator functions, and will measure the detect and react abilities of a unit equipped with the SIMS and interoperating with the Tier 2 CNDSP, NCDOC. Because of the complexity of the system and the extent of the cyber defense capabilities to be exercised, an extended assessment period is planned (see schedule below.)

During the Adversarial Assessment, the OTA will collect and report, at a minimum, the data in Attachment C of the DOT&E guidance, which requires cyber-trained protect, detect, react, and restore (PDRR) data collectors located in both the local and Tier 2 network defense locations. Where allowed by crew safety or equipment damage concerns, the OTA will directly measure mission effects; otherwise, the OTA will evaluate mission effects using independent subject matter experts and the details of the attacks performed during the Adversarial Assessment. These subject matter experts will consider the effect of the attacks and any demonstrated cyber defender responses on the execution of mission threads and associated system performance parameters.

In the event that the network defenders do not detect malicious network activity, the OTA will inject one or more detection scenarios (white cards) in order to evaluate the reaction and response chain of events.

The OTA will submit the Adversarial Assessment plan for DOT&E approval 90 days prior to execution, and provide a report from the cyber test team along with the data collected in accordance with Attachment C of DOT&E Guidance within 45 days after the assessment.

E.6 Test Limitations

Both the CVPA and AA will be conducted in-port, as the testing will necessarily decertify the platform. Ship's crew will be executing mission threads using simulation data sources to support mission effects data collection during the AA.

If crew safety or equipment damage concerns preclude the evaluation of any systems (e.g., industrial control systems such as PLCs) while onboard the ship, independent laboratory testing of these systems will be performed. This data will be included in the CVPA report and cyber exploitations based on the findings will be white-carded in the AA.

E.7 Schedule *<If the CVPA and AA schedules are not already denoted in the integrated test schedule in the body of the TEMP, they should be included in the Appendix. Multiple CVPA and AA events may be required to support milestone/production decisions.>*

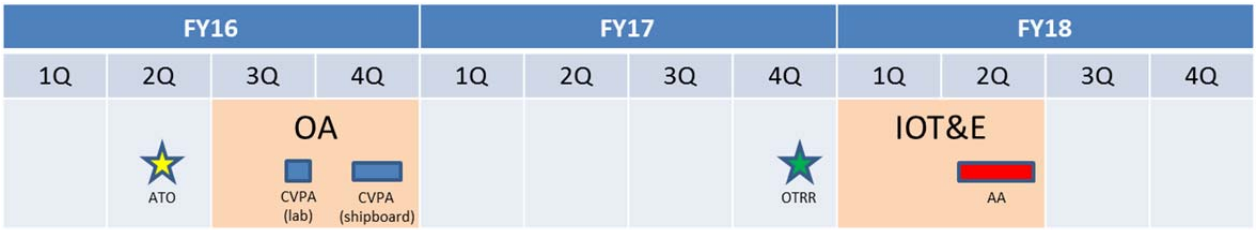

Figure E-2. Cybersecurity Test Schedule

E.8 Resources Resources required for SIMS cybersecurity testing are found in Table E-1. The figures for the NIOC/COMOPTEVFOR CVPA Team and the Naval Research Laboratory include funds for developing advanced cyber exploits against the system, e.g. for PLCs.

Table E-1. SIMS Cybersecurity Test Resources

SUPPORTING UNITS	FY16	FY17	FY18
NIOC/COMOPTEVFOR CVPA Team	$x1		
NIOC/COMOPTEVFOR AA Team			$x2
OTA AA PDRR Data Collection			$x3
OTA Cybersecurity Testing Support	$x4		$x5
Simulation & Instrumentation			$x6
Naval Research Lab Testing Support	$x7		$x8

E.9 Evaluation Structure. The OTA will use the results of SIMS cybersecurity testing, in part, to determine its operational effectiveness, suitability, and survivability. These evaluations should take into account the results of any bench testing. The OTA will assess cybersecurity under Critical Operational Issue X using the following measures:

Table E-2: SIMS Cybersecurity Critical Operational Issue Evaluation Criteria

Criterion	Standard	Minimum Data Required
CyberX.1: Ability to Protect Information and Information Systems	Do the Vulnerabilities and Exploitations discovered during cybersecurity testing of the system put the unit's ability to conduct missions at risk?	DOT&E 2014 Attachments A, B, C
CyberX.2: Ability to Detect Cyber Threat Activity and Malfunctions	Are the accuracy of detections by the SIMS-equipped unit and their defenders during cybersecurity testing sufficient to identify cyber threat activity	DOT&E 2014 Attachments A and C

	or malfunctions that put the unit's ability to conduct missions at risk?	
CyberX.3: Ability to React to Cyber Threat Activity and Malfunctions	Are the mitigation actions provided by the SIMS-equipped unit and their defenders during cybersecurity testing sufficient to ensure the unit's ability to conduct missions following cyber threat activity or malfunctions?	DOT&E 2014 Attachment C
CyberX.4: Ability to Restore System after Cyber Threat Activity or Malfunction	Has the SIMS-equipped unit and their defenders demonstrated the ability to restore normal system operation and conduct missions following cyber threat activity or malfunctions?	DOT&E 2014 Attachments A and C
CyberX.5: Ability to Conduct Missions	Can a SIMS-equipped unit conduct their missions in the presence of malicious cyber threat activity or when encountering malfunctions?	DOT&E 2014 Attachment C
CyberX.6: Ability to Perform Reliably and Be Maintained while also being Secure from Cyber Threat Activity	Can the SIMS-equipped unit perform its mission reliably and perform maintenance in the operational context with a degraded cyberspace environment?	DOT&E 2014 Attachments A, B, and C
CyberX.7: Ability to Preserve System Physical Integrity and the Safety of Operators from Cyber Threat Activity and Malfunctions	In the presence of malicious cyber activity or following a malfunction, is the SIMS able to preserve its own physical integrity and the physical safety of its operators?	DOT&E 2014 Attachments B and C